Internal Controls

Colorado Charter School Institute

CSI Finance

Agenda

- What are Internal Controls?
- Goals/Objectives
- Responsibility
- Framework
- Control Activities
- Monitoring
- Resources

What are Internal Controls?

- Definition:
  - *Internal controls are the mechanisms, rules, and procedures implemented by an organization to ensure the integrity of financial and accounting information, promote accountability and prevent fraud*

Internal Controls – Goals/Objectives

Safeguard Assets

Ensure the reliability and integrity of financial information

Ensure compliance

Promote efficient and effective operations

Accomplishment of organizational goals and objectives

Responsibility

- Management responsibility
  - Maintaining an adequate system of internal control and "setting the tone"
  - Creating financial procedures documenting each process
  - Communicating the expectations and duties of staff in the internal control system
- Staff responsibility
  - Carrying out the internal control activities set forth by management

Framework

Management is responsible for assuring the framework for internal controls is addressed.
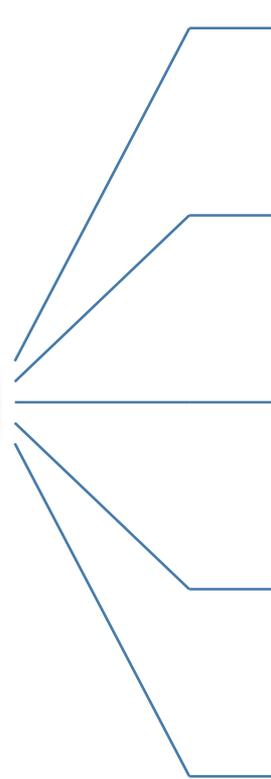
- Control Environment
- Risk assessment
- Monitoring and reviewing
- Information and communication
- Control activities

Framework

- **Control environment**
  - Set of standards, processes, and structures that provide the basis for carrying out internal controls across the organization. – "*Tone at the top*"
  - *Most important element! Without a culture and commitment to internal controls the other elements are unlikely to succeed*

- **Risk assessment**
  - Management should identify which areas pose the greatest risk of inaccuracies and/or loss (i.e. cash management)
  - Biggest risks should receive the greatest amount of effort and level of control

Framework

- **Monitoring and reviewing**
  - The system of internal control should be periodically reviewed by management
    - It is recommended that school leaders review all processes and procedures, including internal controls, *annually*
    - Know that when you apply for renewal, there will be a review of your finance procedures

Framework

- **Information and communication**
  - The availability of information and a clear and evident plan, by school leaders, for communicating responsibilities and expectations is paramount to a good internal control system
    - Staff should receive all applicable policies and procedures, training, and understand their role in each process

Internal Control Activities and Best Practices

- Internal control activities are the *policies and procedures* as well as the daily activities that occur within an internal control system

- A good internal control system should include:
  - ✓Authorization
  - ✓Documentation
  - ✓Reconciliation
  - ✓Security
  - ✓Separation of Duties

Preventive vs. Detective Control Activities

Preventive

- Preventive control activities aim to deter the instance of errors or fraud.
- Preventive activities include thorough *documentation* and *authorization* practices.
- Well thought out processes and procedures that prevent undesirable "activities" from happening

Detective

- Detective control activities identify undesirable "occurrences" after the fact.
- The most obvious detective control activity is reconciliation.

Authorization

- **Definition**: Authorization is the basis by which the authority to complete the various stages of transactions is delegated. These stages include the process of recording (submit), approving, and reconciling.
    - *When developing procedures, authority to perform a specific action should be in line with the designated employees' job description*
- Preventive Activity

Authorization

- Level of authority should be well documented in the schools procedures
  - With each transaction who will:
    - Initiate
    - Submit
    - Approve
    - Reconcile

- Document who has authority to sign checks
  - *A common practice is assigning thresholds*
    - *Example: payments > $5,000 – More then 1 signature will be required*

Authorization Concepts and Best Practice

Key Concept	Best Practice
Level of authority should be documented: Creates an expectation of responsibility and accountability. Authority to perform a particular action may come in hard copy documents or system generated authority (example: system access)	-Policies and procedures within the organization should clearly identify which individuals have authority to initiate, submit, reconcile, view or approve different types of transactions.
Know what you are authorizing: Individuals should have first hand knowledge of the transactions being approved, or they should review supporting documentation to verify the validity and appropriateness of transactions.	-Employees should be properly trained and informed of procedures related to internal controls
Authorization should be timely: Workflow is an important aspect of good internal controls. Time lags between approval and processing provide opportunities for altered documents and potential fraud.	-Many falsifications occur after the approval of a transaction. The workflow process should stress timely authorizations as well as timely processing following approval.

Documentation

- **Definition**: In the context of internal controls, paper or electronic communication which supports the completion of the lifecycle of a transaction. Documentation should include:
    - Evidence for a transaction
    - Who performed each action within a transaction
    - Authority to perform such activities

- Documentation should be kept to reflect all financial activity

Documentation

- Provides financial record of each event or activity

- Should have documentation for all expenses, revenues, inventories, personnel, etc.

- Provides evidence of what transpired as well as information for researching discrepancies

Documentation

- Ensure you are following all state and federal records retention policies

- Do you have more than one copy of your documentation?
  - Scan back up documentation and attach to associated transactions in your accounting software if possible

Documentation Key Concepts and Best Practices

Key Concept	Best Practice
Format of source documents: Well designed documents help ensure the proper recording of transactions. Consistent use of standard forms or templates should be considered whenever possible.	-The advance of online applications provides a fast and efficient method for accessing supporting documentation in a standard format. In other areas, wherever possible, the use of templates provides the same benefits. -Consider creating templates for activities such as: • Email approvals • Time reporting • Reimbursement logs (such as mileage logs, petty cash, others)
Ownership of documents: Documents used to support school business transactions are school property, not the personal property of employees.	-Whenever possible, do not allow employees to take school owned records home. If business needs require school records to be taken home, communicate to employees their responsibility to keep the documents secure, particularly those containing personal information. This is particularly important to communicate to employees that have telecommuting agreements.
Documenting changes: Changes made subsequent to approval of documents should be clear and concise.	-Use attachments or footnotes to document the reasons for corrections/adjustments to any records. Make the time/date and the approval of such corrections/adjustments clear and evident.

Documentation Key Concepts and Best Practices

Key Concept	Best Practice
Avoid duplicate processing: Establish a method to avoid duplicate processing, especially in regards to transactions that result in payments to individuals such as payroll, petty cash and travel reimbursements.	-Build a check for duplicate payments into the processing and approval of payroll, petty cash ,travel reimbursements, and vendor payments. -Create an environment in which all payments are processed in a timely manner. Long delays in processing create opportunities for duplicate payments that go undiscovered. -Look closely at all late entries to watch for double submission of payments. (Example: late timecards, aged vendor invoices, travel expenses requested at a later time separate from the rest of the trip).
Retention: Retention policies exist for all types of supporting documentation. Always keep documents for the appropriate retention period and no longer.	-Establish a process for purging documents that have reached the end of their retention period. Document who, when and how each record type should be purged. -Be aware of record retention responsibilities.

Reconciliation

- **Definition**: Reconciliation is the process of comparing transactions and activity to supporting documentation. It involves resolving any discrepancies that may have been discovered.

- **Purpose**: The process of reconciliation ensures the accuracy and validity of financial information. Also, a proper reconciliation process ensures that unauthorized changes have not occurred to transactions during processing.

Reconciliation

- Reconciliations should be completed by someone who is not involved in the associated process
  - *Example (1): Employee involved with cash receipts should not reconcile bank statements*
  - *Example (2): Employee who reconciles fixed asset inventory to ledger should not have access to the physical inventory*

Reconciliation Key Concepts and Best Practices

| Key Concept	Best Practice
Accuracy of activity: A good internal control system provides a mechanism to verify that transactions and activity are for the correct purpose and amount, and allowable.	-For each type of activity consider documenting the particular information from source documents that is to be compared to the appropriate report. This assists to ensure that transactions are valid and are correct in purpose. (example: determine that for travel reimbursement source documents, the traveler name, destination, purpose of the trip, etc. will be matched to the monthly financial report) -Ensure that transactions have been properly authorized. Especially, if the source documents are paper based, review for potential changes to the document between approval and processing of transactions. -Ensure that all transactions are allowable.
Errors correction: Errors and discrepancies, intentional or unintentional, should be detected, investigated and resolved in a timely fashion.	-If an error or discrepancy is identified between a report and source documentation, follow up with the appropriate central office or processing department to seek clarification. A journal entry or other action may be needed to resolve the issue.

Reconciliation Key Concepts and Best Practices

Key Concept	Best Practice
Matching to the source: The oversight of any transaction is strengthened by the process of matching source documentation of the transaction to the appropriate reporting documentation or reporting tool.	-Comparing board approved budgets to actual revenues and expenditures is one example of using the appropriate reporting tool in reconciling transactions. Any discrepancies found can be researched to the source documentation.
Documenting the process and completion: Reconciliation processes are most effective when they are consistent and thorough. Employees involved in the reconciliation process should be knowledgeable and clear on their responsibilities and expectations. It should be clear to an external reviewer when a reconciliation has been completed.	-Be consistent with reconciliation processes. Changing the reconciliation process often leads to undiscovered inaccuracies and potential fraud. -Reconciliation should be documented clearly to verify that a review has been done. (reviewed by and date) -The reconciliation process and procedures should be documented clearly and communicated. Consider documenting: 1. The steps in the process 2. Who performs each step 3. Expectation regarding timeliness 4. A mechanism for providing proof that all activity has been reviewed and reconciled 5. A procedure for error correction

Security

The security of school assets and records includes 3 types of safeguards:

Administrative: Focuses on process put in place to protect assets/records

Physical: Protection of physical records and assets from loss by theft or damage

Technical: Protection of electronic records from loss by theft, damage, or loss in transport
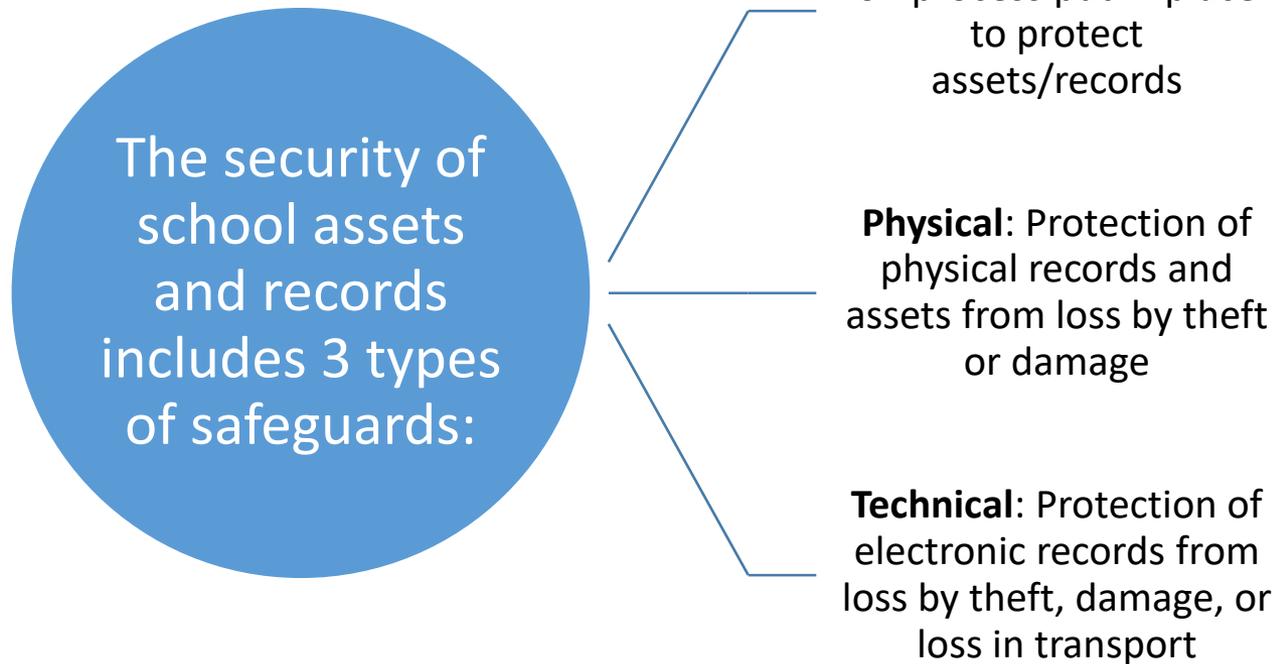
Security

- **Purpose**: Assets and records (physical and electronic) should be kept secure at all times to prevent unauthorized access, loss, or damage. The security of assets and records is essential for ongoing operations, accuracy of information, privacy of personal information included in some records and in many case state or federal law.

Security – Examples

- File cabinets should be locked at all times

- Limit access to records and assets to those who have been authorized and have a business need for them

- Setup password protected access to electronic records

- Develop a prescribed standard for creating passwords

Security Key Concepts and Best Practices

Key Concept	Best Practice
Designate a point person	-Designating a point person for all areas or individually for the 3 types of security provides an established responsibility and accountability for proper security procedures
Administrative organization	-Keep an up-to-date organizational chart that defines the reporting relationships as well as responsibilities, including back-up responsibilities, regarding internal controls within the school.
Access to electronic records: Limit access to records and assets to those who have been authorized and have a business need for them	-Establish and communicate standards for screensavers and password protected screens. -Setup password protected access to electronic records. -Do not allow electronic records to be downloaded to mobile workstations and transported outside of the office.
Physical access to records and assets: Limit access to records and assets to those who have been authorized and have a business need for them.	-Keep file cabinets locked and secure -Ensure unused assets are stored in a secure location (i.e. laptops etc.)
Employee turnover: Limit access to records and assets to those who have been authorized and have a business need for them.	-Develop a checklist for removing access to records upon separation of an employee. Develop a process and assign a point person the responsibility of administering the process for deleting access to records.
Passwords:	-Have a prescribed standard for departmental passwords. Make them complex and enforce a policy for changing passwords periodically.

Separation of Duties
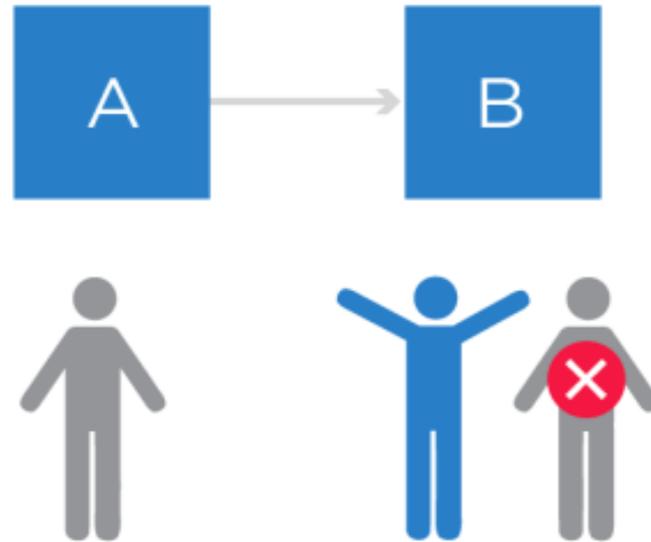
Separation of Duties

- **Definition**: Separation of duties is the means by which no one person has sole control over the lifespan of a transaction. Ideally, no one person should be able to initiate, record, authorize and reconcile a transaction.
  - *Document employee responsibilities!*
- **Purpose**: The separation of duties assures that mistakes, intentional or unintentional, cannot be made without being discovered by another person.

Separation of Duties Key Concepts and Best Practices

Key Concept	Best Practice
School differences: Separation of duties may vary depending on the size of the organization and structure	-Duties may be separated by department or by individuals within a department. The level of risk associated with a transaction should come into play when determining the best method for separating duties.
Demonstration: Separation of duties should be able to be demonstrated to an outside party.	-Documentation of processes and authorization is helpful in demonstrating a system of control that includes separation of duties.
Document the responsibilities: Separation of duties should be clearly defined, assigned and documented.	-Document and clearly communicate who will initiate, submit, process, authorize, review and/or reconcile each activity within the unit.
Review and oversight: Management should increase the review and oversight function when it is difficult to sufficiently separate duties.	-Assess the potential for mistakes or fraudulent transactions. If the separation of duties is not sufficient to eliminate or adequately reduce the risk of discovering errors, the level of review of management should be increased over the particular activity.

Continued Monitoring

- With a good internal control system in place, other considerations to keep in mind include:
  - Regularly communicate updates and reminders of policies to staff through emails, staff meetings, etc.
  - Periodically assess risks and the level of internal control required to protect school assets and records related to those risks.
  - Management is responsible for making sure that all staff are familiar with school policies and changes in those policies.

Final Thoughts

Elaborateness of system is a matter of judgement on the part of management

Always include careful consideration for circumstances, such as:

- The size of the organization
- The number of personnel available
- The relationship between the costs and benefits of designing and implementing controls

In addition, the nature of internal control is such that appropriate methods and systems will not guarantee that an organization's objectives will be achieved!

- What kind of assurance do good internal controls provide?
  - a. None
  - b. Reasonable
  - c. Absolute

Scenario One

- Employee A receives an invoice for payment and notices the vendor is not yet set up as a vendor in the system. After receiving a W-9 employee A sets up the vendor in the accounting system. After invoice has proper approvals, Employee A enters the invoice into the system for payment.

- Any issues with this scenario?

Scenario Two

- When assets are purchased Employee A is responsible for tagging and recording the assets into the asset log when received. All unused IT equipment is secured in a locked area for which Employee A has been granted access. Access has been granted to this employee so they can easily reconcile the assets on hand to the schools asset log.

- Any issues with this scenario?

Scenario Three

- ***Employee A:*** receives all cash and/or checks received in the front office, records the activity into the accounting system and creates a deposit slip

- ***Employee B:*** completes deposit at bank

- ***Employee C:*** completes a monthly reconciliation of the bank statement to accounting system and back up

- Any Issues with this scenario?

Scenario Four

- Employee A was assigned a procurement card to make small dollar purchases such as office supplies, etc. At the close of each month, the employee compiles what back up they can find, and files the monthly card statement with this back up in a secure filing cabinet.

- Any Issues with this scenario?

Scenario Five

- Employee A was assigned a procurement card for use on small purchases. The card is shared and utilized by multiple staff members for various purchases as needed. The card is kept in a secure location that only employees can access.

- Any Issues with this scenario?

Resources

- State records management manual for school districts:
- https://www.colorado.gov/pacific/archives/school-records-management

- CDE Financial Policies and Procedures Handbook
- http://www.cde.state.co.us/cdefinance/fpphandbook

Questions?

COLORADO
CHARTER SCHOOL INSTITUTE